**Secure Vehicle-to-Vehicle Communication with Identity-Based Cryptography Using License Plate Recognition**

A major project report submitted in partial fulfillment of the requirement for the award of degree of

**Bachelor of Technology**

in

**Computer Science & Engineering**

*Submitted by*

**Pourush Pandey (221030172)**

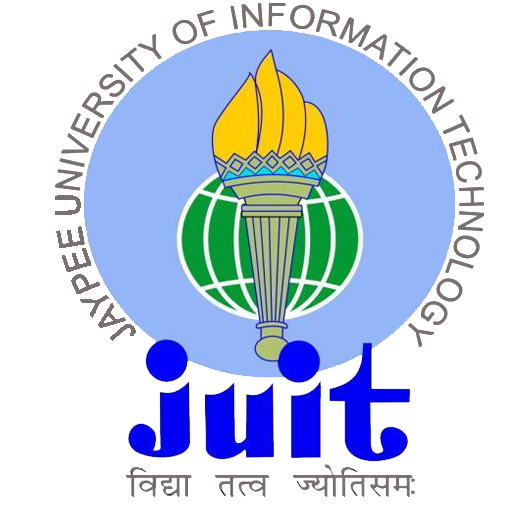
**Akankshita Puri (221030052)**

**Adarsh Mishra (221030386)**

**Avinav Jay (221030062)**

*Under the guidance & supervision of*

**Dr. Nishant Sharma**



**Department of Computer Science & Engineering and**

**Information Technology**

**Jaypee University of Information Technology, Waknaghat, Solan - 173234 (India)**

**December 2025**

# 

# Table of Contents

[**Table of Contents**](#_fao8mgfcpevl) **ii**

[**List of Figures**](#_l1ss6ayzqd9m) **iii**

[**List of Abbreviations, Symbols or Nomenclature**](#_f093am6we3l9) **iv**

[**Abstract**](#_ivbyebw8cm43) **v**

[**Chapter 1: Introduction 1**](#_v928u2b11c16)

[1.3 Objectives 2](#_qmva4el0mwvw)

[1.4 Significance and Motivation of the Project Work 3](#_syiefo6h9zty)

[1.5 Organization of Project Report 4](#_a2fvgo3x9xhm)

[Chapter 1: Introduction 4](#_lq5ezx91pztl)

[Chapter 2: Literature Survey 5](#_s2dw9gioid70)

[Chapter 3: System Development 5](#_3qagjj78sgd)

[**Chapter 2: Literature Survey 7**](#_mckzliqw2t10)

[2.1 Overview of Relevant Literature 7](#_elkag3puho1x)

[License Plate Recognition (LPR) Evolution: 7](#_gjku1w22418e)

[Vehicle-to-Vehicle (V2V) Communication & Security: 8](#_vsfyf8vat98z)

[Integration of LPR and V2V: 8](#_h7j6d0uecl8b)

[2.2 Key Gaps in the Literature 8](#_gq7mmhnxqpig)

[**Chapter 3: System Development 10**](#_snpt4zwbpepu)

[3.1 Requirements and Analysis 10](#_trljpu76b82)

[Functional Requirements 10](#_dz67nz9elu3i)

[Non-Functional Requirements 11](#_un9t8dbebn2n)

[Requirement Analysis 11](#_d5lqqk6m6l3e)

[3.2 Project Design and Architecture 12](#_2ghnll8t82u)

[1. License Plate Recognition Layer 12](#_w3nkzk7fj1qc)

[3. Communication Layer 12](#_i4ey1axsq61)

[4. Application Layer 12](#_if7hodaao395)

[5. High-Level System Architecture Diagram 13](#_f1qs6tzedapf)

# List of Figures

1. Figure 3.1: High-Level System Architecture of Secure V2V Communication Framework integrating License Plate Recognition (LPR), Identity-Based Cryptography (IBC), and multi-platform applications.

## 

## List of Abbreviations, Symbols or Nomenclature

| **Abbreviation** | **Full form** |
| --- | --- |
| V2V | Vehicle-to-Vehicle |
| VANET | Vehicular Ad-hoc Network |
| ITS | Intelligent Transportation System |
| IBC | Identity-Based Cryptography |
| PKI | Public Key Infrastructure |
| PKG | Private Key Generator |
| LPR | License Plate Recognition |
| OCR | Optical Character Recognition |
| CNN | Convolutional Neural Network |
| RNN | Recurrent Neural Network |
| UI | User Interface |
| API | Application Programming Interface |

## 

## Abstract

Vehicular Ad-hoc Networks (VANETs) are critical to Intelligent Transportation Systems (ITS), enabling vehicles to exchange safety alerts, traffic information, and cooperative driving data in real time. However, ensuring secure, scalable, and low-latency communication in dynamic vehicular environments remains a challenge, especially with conventional Public Key Infrastructure (PKI) approaches that suffer from high certificate management overhead and limited scalability.

This project proposes a novel framework for secure Vehicle-to-Vehicle (V2V) communication that integrates **License Plate Recognition (LPR)** with **Identity-Based Cryptography (IBC)**. In this system, license plate numbers serve as unique cryptographic identities, enabling certificate-free public key derivation. A **Private Key Generator (PKG) portal**, implemented as a web application for traffic authorities, issues and manages private keys, while a **driver-facing mobile application** performs real-time license plate recognition, encryption, and decryption of messages.

The multi-layered architecture consists of (i) LPR layer for vehicle identity extraction, (ii) cryptographic layer for key generation and secure messaging, (iii) communication layer for authenticated V2V data exchange, and (iv) application layer with mobile and web interfaces. This design ensures authenticity, confidentiality, integrity, and scalability of vehicular communication.

The expected outcomes include reduced certificate overhead, improved real-time authentication, and stronger resilience against impersonation, replay, and spoofing attacks, thereby contributing to safer and more reliable intelligent transportation networks.

## 

## Chapter 1: Introduction

**1.1 Introduction**

Vehicular Ad-hoc Networks (VANETs) have become a critical component of **Intelligent Transportation Systems (ITS)**, enabling real-time **Vehicle-to-Vehicle (V2V) communication**. Through these networks, vehicles can exchange vital information such as **safety alerts, traffic updates, crash warnings, and cooperative driving data**, which enhances road efficiency and reduces the risk of accidents. VANETs are therefore essential for the development of **smart cities and autonomous transportation systems**, where timely and reliable information sharing can directly impact road safety and traffic management.

Despite their benefits, VANETs face significant **security challenges**. Threats such as **impersonation attacks, message tampering, replay attacks, and unauthorized access** can compromise both vehicles and passengers. Traditional **Public Key Infrastructure (PKI)-based solutions** offer strong cryptographic protection but come with high overheads in **certificate management, distribution, and revocation**, as well as increased communication latency. These limitations make PKI less practical in highly dynamic vehicular environments, where real-time authentication and scalability are critical.

To overcome these challenges, **Identity-Based Cryptography (IBC)** provides a certificate-free alternative, allowing unique vehicle identifiers, such as **license plate numbers**, to function directly as cryptographic keys. When integrated with **License Plate Recognition (LPR) systems** based on **computer vision and deep learning**, vehicles can be accurately identified and authenticated in real time. This approach enables a **secure, scalable, and efficient V2V communication framework**, while also supporting mobile applications for drivers and web platforms for traffic authorities to monitor, register, and authenticate vehicles in the network.

**1.2 Problem Statement**

With the rapid rise of connected and autonomous vehicles, ensuring **secure and reliable communication** in Vehicular Ad-hoc Networks (VANETs) has become a critical concern. Current **Vehicle-to-Vehicle (V2V) communication systems** remain vulnerable to a wide range of cyber threats, including **spoofing, Sybil attacks, replay attacks, and false data injection**. These attacks not only compromise the integrity and authenticity of transmitted data but also pose significant risks to **road safety, traffic efficiency, and passenger security**. As vehicles increasingly rely on real-time information sharing for collision avoidance, route optimization, and cooperative driving, even minor security breaches can lead to catastrophic consequences on the roads.

While **Public Key Infrastructure (PKI)-based approaches** have been widely adopted to address these security challenges, they suffer from several limitations in practical deployment. The process of **certificate generation, distribution, revocation, and management** introduces substantial overhead, especially in **highly dynamic vehicular environments** where vehicles frequently join and leave the network. This leads to **latency in authentication and verification**, which can undermine the effectiveness of real-time V2V communication. Additionally, conventional PKI frameworks often struggle to scale efficiently across large vehicular networks, making them less suitable for emerging intelligent transportation systems.

Another significant limitation of existing V2V systems is the lack of integration between **vehicle identification mechanisms** and cryptographic frameworks. Most current solutions treat vehicle authentication and identity verification as separate processes, leading to inefficiencies and potential vulnerabilities. There is a pressing need for a **unified system** that links a vehicle’s **physical identity**, such as its **license plate**, with secure cryptographic mechanisms. Such an approach would allow vehicles to be uniquely and verifiably identified in real time, enabling **trustworthy communication**, reducing the risk of impersonation attacks, and improving overall network reliability. Developing this integrated framework is essential for creating **scalable, secure, and efficient V2V communication systems** capable of supporting the growing demands of modern intelligent transportation networks.

### 1.3 Objectives

.

The project is designed to address the challenges associated with secure Vehicle-to-Vehicle (V2V) communication by pursuing the following specific objectives:

**1.3.1** To design and deploy a **certificate-free V2V communication protocol** using **Identity-Based Cryptography (IBC)** in order to eliminate the overhead of certificate management and ensure secure communication between vehicles.

**1.3.2** To implement a **License Plate Recognition (LPR) system** based on **computer vision and deep learning algorithms**, capable of accurately extracting vehicle identities in real time under dynamic road conditions.

**1.3.3** To integrate the recognition module with the cryptographic system, thereby enabling vehicles to communicate securely using their **license plate-derived identities**.

In addition to these core objectives, the project also seeks to:

a) Develop a **mobile application** for drivers that enables seamless vehicle registration, authentication, and participation in the secure V2V communication network.

b) Create a **web-based platform for traffic authorities** to efficiently monitor, register, and authenticate vehicles within the network.

c) Evaluate the proposed system in terms of **security strength, latency, and scalability**, and compare its performance against conventional PKI-based solutions to demonstrate its effectiveness.

### 1.4 Significance and Motivation of the Project Work

The rapid proliferation of connected and autonomous vehicles has transformed conventional transportation systems into intelligent, interconnected ecosystems. Vehicular Ad-hoc Networks (VANETs) form the backbone of this transformation by enabling real-time Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication. These networks facilitate the exchange of crucial data such as accident warnings, traffic congestion updates, road hazard notifications, and cooperative driving decisions, thereby improving both safety and efficiency on modern roads.

However, the full potential of VANETs is challenged by security vulnerabilities that expose vehicles to impersonation, spoofing, Sybil attacks, replay attacks, and false data injection. These attacks threaten not only the reliability of communication but also the safety of passengers and other road users. While Public Key Infrastructure (PKI)-based solutions have been widely adopted for securing vehicular communication, they impose significant drawbacks in highly dynamic vehicular environments. PKI requires constant certificate distribution, verification, and revocation management, which introduces high overhead, increased latency, and limited scalability.

This motivates the exploration of **Identity-Based Cryptography (IBC)** as an alternative. IBC eliminates the need for digital certificates by using unique, easily verifiable vehicle identifiers (such as license plates) as cryptographic public keys. This approach simplifies trust establishment while ensuring security and scalability. The integration of **License Plate Recognition (LPR)** powered by computer vision and deep learning provides an automated mechanism to extract vehicle identities in real time, thereby linking physical vehicle identity with cryptographic operations.

The significance of this project lies in its holistic approach:

* It bridges the gap between vehicle identification technologies and secure communication frameworks.
* It enhances trustworthiness and scalability in VANETs by combining LPR with IBC.
* It reduces certificate management overhead while maintaining strong cryptographic security.
* It offers practical utility through the development of a driver mobile application and a traffic authority monitoring platform, enabling secure registration, monitoring, and authentication of vehicles.

Ultimately, this project is motivated by the pressing need to strengthen the security of V2V communications while ensuring low latency, high scalability, and strong resilience against cyber threats. Its successful implementation contributes directly to safer intelligent transportation systems, paving the way for reliable autonomous and connected vehicle ecosystems.

### 

### 1.5 Organization of Project Report

The project report is structured into distinct chapters to ensure systematic presentation of the work undertaken. Each chapter addresses specific aspects of the project and is organized in alignment with the institutional guidelines. The overall organization is as follows:

#### Chapter 1: Introduction

This chapter provides the foundation of the report by introducing the context, background, and motivation for the project. It is divided into the following sections:

* 1.1 Introduction Offers a general overview of Vehicular Ad-hoc Networks (VANETs), their role in intelligent transport systems, and the need for secure Vehicle-to-Vehicle (V2V) communication.
* 1.2 Problem Statement Defines the challenges associated with current PKI-based vehicular communication frameworks, including scalability issues, certificate management overhead, and vulnerability to various cyber-attacks.
* 1.3 Objectives Enumerates the main goals of the project, such as developing a certificate-free IBC-based V2V protocol, implementing an LPR system, integrating the two into a secure communication framework, and testing system performance.
* 1.4 Significance and Motivation of the Project Work Explains the importance of the project in addressing cybersecurity challenges in connected vehicles, highlighting how the proposed approach improves scalability, reduces latency, and enhances security compared to conventional PKI.
* 1.5 Organization of Project Report Outlines the structure of the report (this section itself), giving readers a roadmap of subsequent chapters.

#### Chapter 2: Literature Survey

This chapter provides an overview of the existing research in the area of vehicular communication security, identity-based cryptography, and license plate recognition. The focus is on identifying the current state of the art, as well as the research gaps addressed by this project. It contains the following sections:

* 2.1 Overview of Relevant Literature Summarizes prior studies from standard books, research journals, conference papers, technical white papers, and reputable online resources, with special emphasis on the last five years. It reviews existing PKI-based approaches, identity-based cryptographic protocols, and recent advancements in deep learning-based license plate recognition.
* 2.2 Key Gaps in the Literature Highlights the shortcomings of existing systems, such as the lack of integration between physical vehicle identifiers and cryptographic systems, certificate management challenges in PKI, and limited real-time applicability of current LPR solutions. This section provides the rationale for proposing a unified IBC-LPR framework.

#### Chapter 3: System Development

This chapter presents the development aspects of the proposed solution, focusing on system requirements, design, and overall architecture. It is organized into the following sections:

* 3.1 Requirements and Analysis Defines the functional and non-functional requirements of the system. Functional requirements include secure V2V communication, real-time license plate recognition, and identity-based authentication. Non-functional requirements include low latency, scalability, and robustness against cyber-attacks.
* 3.2 Project Design and Architecture Explains the high-level system architecture, including the integration of the License Plate Recognition (LPR) module with the Identity-Based Cryptography (IBC) protocol. It also describes the design considerations for the mobile application (for drivers) and the web platform (for traffic authorities). Diagrams such as data flow diagrams, use-case diagrams, or system architecture diagrams may be included here to enhance clarity.

## 

## Chapter 2: Literature Survey

### 2.1 Overview of Relevant Literature

License Plate Recognition (LPR) and Vehicle-to-Vehicle (V2V) communication technologies have seen tremendous development over the last ten years, evolving from traditional image processing and cryptographic approaches to high-end deep learning-based recognition and identity-based secure communication architectures.

#### License Plate Recognition (LPR) Evolution:

Early LPR technologies were based primarily on traditional image processing methods like edge detection, histogram equalization, contour extraction, and OCR-based character segmentation (Chang et al., 2004). Although these approaches found good accuracy under controlled conditions, they were sensitive to changes in lighting, viewing angle, environmental conditions, and plate occlusion. With the introduction of classical machine learning algorithms in the mid-2010s, namely SVM and k-NN, character recognition improved but demanded lots of manual feature engineering and did not handle non-standard or multilingual plates well. Research appearing in IEEE Transactions on Intelligent Transportation Systems (2018–2022) suggests that although these approaches enhanced the accuracy of recognition, their robustness in cluttered urban and dynamic traffic conditions was still limited.

Deep learning integration significantly improved the capabilities of LPR. CNN-based architectures feature extraction is automated, allowing accurate plate localization and recognition even in adverse environmental conditions. Research like Ahmed et al. (2023) and Pooja et al. (2025) illustrated that a combination of YOLOv5/YOLOv8 with light-weight OCR processors (EasyOCR/Tesseract) provides real-time recognition at over 95% accuracy on various datasets, such as multi-angle and occluded plates. Additional advancements involving RNNs, LSTMs, and transformer-based sequence models enable segmentation-free recognition, enhancing performance on distorted or low-res plates. These methods have been validated on data like OpenALPR, IIT Delhi car plates, and multi-national plate collections, demonstrating region/language generalizability.

Edge computing has come to be an essential part to manage latency and computation load in real-time LPR applications. Embedded solutions such as NVIDIA Jetson, Raspberry Pi, and FPGA boards support on-device processing, essential for automated tolling systems, parking systems, and surveillance, as applied by Liu et al. (2022). This reduces cloud computing dependency and supports real-time, low-latency decision-making in congested areas.

#### Vehicle-to-Vehicle (V2V) Communication & Security:

Secure V2V communication is essential for connected vehicles and smart transport systems. Rathore et al. (2022) identify the common cyber attacks like spoofing, Sybil attacks, and replay attacks that jeopardize vehicular safety and integrity of data. Conventional PKI-based approaches provide robust security but have scalability and certificate management problems in extremely dynamic vehicular networks.

Identity-Based Cryptography (IBC) provides a promising approach. Shamir (1984) proposed the generation of cryptographic keys from identifiers, which serves as the basis for secure authentication in V2V communication. Qiang Li (2023) employed an identity-based authentication and key agreement protocol using vehicle-specific identifiers like license plate numbers for key generation. This method minimizes overhead, facilitates scalability, and provides secure real-time communication among vehicles, serving as a strong theoretical and practical foundation for merging ANPR with V2V security.

#### Integration of LPR and V2V:

Recent studies show partial integration of ANPR and secure vehicular communications. Ahmed et al. (2023) used ML-based ANPR for real-time vehicle management, whereas Ramya & Vekata (2021) investigated the use of ML for collision avoidance and safety. Sultan et al. (2023) discussed recognition in adverse environmental conditions. Yet there are few fully integrated systems that integrate real-time ANPR with identity-based V2V authentication, which provides a huge opportunity for practical implementation in smart transportation systems.

### 2.2 Key Gaps in the Literature

Even with the considerable advancement in Automatic License Plate Recognition (LPR) and Vehicle-to-Vehicle (V2V) security, there are still some voids present that restrict their application effectiveness in real-life scenarios. The foremost difficulty is the absence of unification between LPR and V2V security. These two fields are usually handled separately in existing research: LPR is concerned with precise and speedy vehicle detection, and V2V research is centered on authentication, encryption, and secure communication. No single approach solves effectively the problem of unifying license plate data with identity-based cryptography in real-time authentication of vehicles. In the absence of this integration, smart transport systems cannot take full advantage of vehicle-specific identifiers to facilitate security, and their practical application in complex urban settings is thereby restricted.

Another major deficiency is environmental robustness. Even with sophisticated CNN and YOLO-based LPR algorithms, the performance of recognition drastically degrades in difficult situations like low-light or night time, bad weather, motion blur, and partial occlusions by dirt, stickers, or other cars. While deep learning methods have enhanced robustness, more studies are required to make systems robust against such real-world scenarios. Methods such as multi-spectral imaging, advanced preprocessing, and smart data augmentation may assist models in managing variations in weather, lighting, and occlusions more efficiently.

Scalability and computational efficiency also present significant challenges. Deep learning models requiring high accuracy are usually computationally intensive, needing GPUs or cloud processing, and thus not suitable for edge devices such as parking gates, toll booths, or traffic cameras. Lightweight deployment approaches usually sacrifice accuracy for speed, but high-accuracy real-time recognition is challenging. Furthermore, the majority of studies, when they do validate their models, test on controlled or small datasets and leave open questions regarding performance when deployed city-wide in heavy traffic. There is still research necessary on optimized architectures, model pruning, quantization, distributed edge-cloud systems, and efficient load balancing to support large-scale deployment.

Lastly, there is a lack of dataset diversity and security connection. Most available LPR datasets have restricted geographic coverage, plate types, and weather conditions, affecting model generalization. Moreover, despite the availability of V2V identity-based cryptography, not many systems utilize real-time LPR as a part of the authentication system. This restricts the option to link direct physical vehicle identity with cryptographic credentials, making LPR and V2V systems underutilized in holistic smart city systems. Filling these gaps will be important in creating robust, secure, and scalable future intelligent transportation systems.

## 

## Chapter 3: System Development

### 3.1 Requirements and Analysis

### Functional Requirements

1. Vehicle-to-Vehicle Secure Communication
   * Vehicles must be able to exchange authenticated and encrypted messages in real time.
   * Communication should be identity-based, using the license plate as the unique cryptographic identity.
2. License Plate Recognition (LPR)
   * The system should capture and process vehicle images to extract the license plate.
   * The recognized plate should be used to derive the cryptographic identity of the vehicle.
3. Cryptographic Implementation  
   * Implement Identity-Based Cryptography (IBC) for secure key generation and message encryption/decryption.
   * Ensure lightweight and scalable cryptographic operations suitable for mobile and web platforms.
4. Mobile Application  
   * Provide a driver-facing mobile app to enable secure message exchange, warnings, and alerts.
   * The app integrates cryptographic functions and offers an intuitive interface.
5. Web-Based Application  
   * Provide an admin/authority-facing web application to register vehicles, monitor communication, and manage keys.
   * Include dashboards for real-time oversight of V2V communications.

### Non-Functional Requirements

* Security: Robust protection against spoofing, replay attacks, and unauthorized access.
* Scalability: Must handle a large number of vehicles communicating simultaneously.
* Performance: Real-time communication with minimal latency.
* Interoperability: Compatibility across different mobile devices and web browsers.
* Usability: Simple interfaces for both drivers and administrators.

### Requirement Analysis

Traditional PKI systems are not well-suited for V2V networks due to certificate management overhead and scalability issues. The proposed system overcomes these issues by:

* Using license plates as inherent identities, eliminating external certificate authorities.
* Leveraging IBC to generate public/private keys dynamically from identities.
* Integrating computer vision (LPR) with cryptographic modules, ensuring automated and secure identity mapping.
* Combining mobile and web applications to cover both end-user (drivers) and administrative (authorities) needs.

## 3.2 Project Design and Architecture

The system is designed as a multi-layered architecture consisting of the following components:

### 1. License Plate Recognition Layer

* Input: Vehicle license plate image.
* Processing: Image preprocessing → character segmentation → OCR (Optical Character Recognition).
* Output: Extracted license plate string, which is passed to the cryptographic module.

**2. Cryptographic Layer (IBC-Based)**

* Takes the license plate string as the **unique identity**.
* **Public Key:** Derived directly from the license plate (identity) through **mobile app**.
* **Private Key:** Securely generated and distributed by the **PKG** portal **web app**.
* Vehicles use these keys to encrypt and decrypt V2V messages.
* Ensures **authenticity, confidentiality, and integrity** of all communications.

### 3. Communication Layer

* Implements secure protocols for real-time V2V data exchange.
* Supports warning broadcasts (collision alerts, traffic status).
* Handles encryption/decryption seamlessly for both mobile and web endpoints.

### 4. Application Layer

* Mobile Application (Drivers):
  + Integrates with the LPR module to detect surrounding vehicles’ license plates.
  + Uses IBC to encrypt outgoing messages and decrypt received ones using its issued private key.
  + Provides a real-time user interface for drivers to send/receive alerts.
* Web Application (Authorities):
  + Acts as PKG portal for key management including issuance and revocation,.
  + Offers dashboards for monitoring communication, vehicle registration, and security audits

### 5. High-Level System Architecture Diagram

**Figure 3.1** : High-Level System Architecture of Secure V2V Communication Framework integrating License Plate Recognition (LPR), Identity-Based Cryptography (IBC) and multi-platform applications.

